PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-156771
(43)Date of publication of application : 08.06.2001

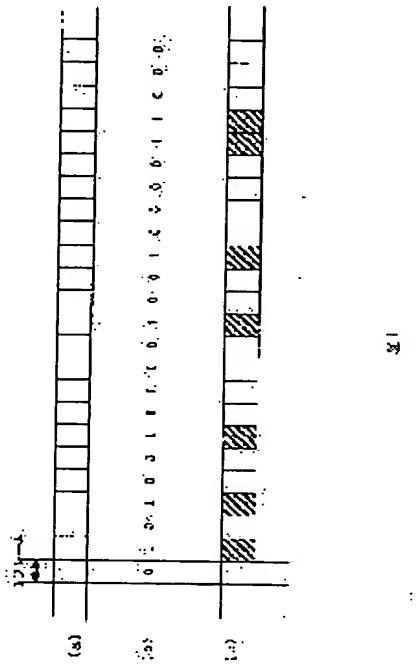
(51)Int.Cl. H04L 9/16
G06F 12/14
H04L 9/18

(21)Application number : 11-339523
(22)Date of filing : 30.11.1999

(71)Applicant : VICTOR CO OF JAPAN LTD
(72)Inventor : KOHARI HARUKUNI

(54) ENCRYPTED INFORMATION TRANSMISSION METHOD, ENCRYPTED INFORMATION TRANSMITTER AND TRANSMISSION MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an encrypted information transmission method that can strongly prevent illegal use of contents information even in the case that a transmission stream is partially encrypted and to provide a transmitter and a transmission medium.
SOLUTION: An audio or image stream is encrypted at random in the unit of frames on the basis of a random number and the encrypted stream is transmitted. Since flag information or the like denoting which stream is encrypted or not is not provided in the stream, the security strength against the illegal use of contents can be much more enhanced than that of a conventional partial encryption method.



LEGAL STATUS

[Date of request for examination] 26.04.2002
[Date of sending the examiner's decision of rejection] 15.04.2005
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）

(11)特許出願公開番号
特開2001－156771
（Ｐ２００１－１５６７７１Ａ）
(43)公開日　平成13年６月８日(2001.6.8)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード（参考）
H04L 9/16		G06F 12/14	320	B 5B017
G06F 12/14	320	H04L 9/00	643	5J104
H04L 9/18			651	

審査請求　未請求　請求項の数10　ＯＬ　（全７頁）

(21)出願番号　特願平11－339523

(22)出願日　平成11年11月30日(1999.11.30)

(71)出願人　000004329
日本ビクター株式会社
神奈川県横浜市神奈川区守屋町３丁目12番地

(72)発明者　小張　晴邦
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内

Ｆターム(参考)　5B017 AA07 BA05 BA07 BB02 BB03
CA06 CA09 CA16
5J104 AA01 AA16 AA33 EA04 EA25
JA04 NA02

(54)【発明の名称】暗号化情報伝送方法、暗号化情報伝送装置、及び伝送媒体

(57)【要約】
【課題】　伝送ストリームを部分的に暗号化する場合においても、コンデンツ情報の不正使用を強力に防止できる暗号化情報伝送方法、伝送装置、及び伝送媒体を提供すること。
【解決手段】　音声または画像ストリームは、乱数値に基づきフレーム単位でランダムに暗号化され伝送される。どのフレームが暗号化されているか否かを示すフラッグ情報などをストリーム内に設けていないので、コンテンツの不正使用に対する安全強度を、従来の部分的な暗号化方法よりも高めることができる。

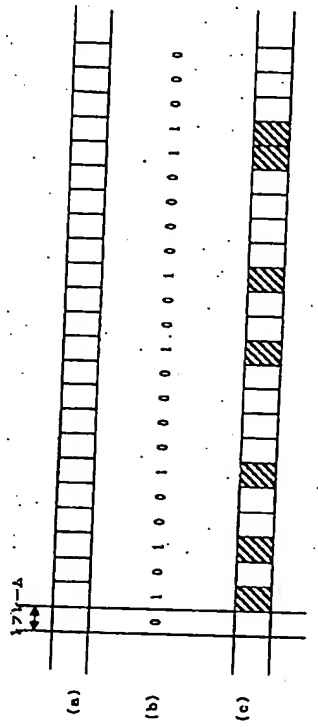


図1

1

【特許請求の範囲】

【請求項１】複数のフレームからなるストリームに対し、所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとを決定し、暗号化を行うと決定されたフレームのデータを各フレーム単位で暗号化してストリームを伝送することを特徴とする暗号化情報伝送方法。

【請求項２】複数のフレームからなるストリームに対し、所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとを決定し、暗号化を行うと決定されたフレームのデータを各フレーム単位で暗号化すると共に、前記所定の生成多項式の情報を暗号化した生成多項式暗号化情報を付加してストリームを伝送することを特徴とする暗号化情報伝送方法。

【請求項３】複数のフレームからなるストリームに対し、所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとを決定し、暗号化を行うと決定されたフレームのデータを各フレーム単位で暗号化すると共に、前記所定の生成多項式の情報を暗号化した生成多項式暗号化情報と、前記所定の生成多項式の乱数発生のための複数の初期値の情報を暗号化した初期値暗号化情報とを付加してストリームを伝送することを特徴とする暗号化情報伝送方法。

【請求項４】複数のフレームからなるストリームに対し、所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとを決定し、暗号化を行うと決定されたフレームのデータを各フレーム単位で暗号化してストリームを伝送することを特徴とする暗号化情報伝送装置。

【請求項５】複数のフレームからなるストリームに対し、所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとを決定し、暗号化を行うと決定されたフレームのデータを各フレーム単位で暗号化すると共に、前記所定の生成多項式の情報を暗号化した生成多項式暗号化情報を付加してストリームを伝送することを特徴とする暗号化情報伝送装置。

【請求項６】複数のフレームからなるストリームに対し、所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとを決定し、暗号化を行うと決定されたフレームのデータを各フレーム単位で暗号化すると共に、前記所定の生成多項式の情報を暗号化した生成多項式暗号化情報と、前記所定の生成多項式の乱数発生のための複数の初期値の情報を暗号化した初期値暗号化情報とを付加してストリームを伝送することを特徴とする暗号化情報伝送装置。

【請求項７】複数のフレームからなるストリームに対し、所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されたストリームを伝送することを特徴とする伝送媒体。

【請求項８】複数のフレームからなるストリームに対し、所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されると共に、前記所定の生成多項式の情報が暗号化された生成多項式暗号化情報が付加されたストリームを伝送することを特徴とする伝送媒体。

【請求項９】複数のフレームからなるストリームに対し、所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されると共に、前記所定の生成多項式の情報が暗号化された生成多項式暗号化情報と、前記所定の生成多項式の乱数発生のための複数の初期値の情報が暗号化された初期値暗号化情報とが付加されたストリームを伝送することを特徴とする伝送媒体。

【請求項１０】複数のフレームからなるストリームに対し、所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとを決定し、暗号化を行うと決定されたフレームのデータを各フレーム単位で暗号化すると共に、前記所定の生成多項式の乱数発生のための複数の初期値の情報を付加してストリームを伝送することを特徴とする暗号化情報伝送方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、音声や画像等のストリームを暗号化して伝送するための暗号化情報伝送方法、伝送装置、及び伝送媒体に関するものである。そして、この発明は特に、音声や画像等のストリームを部分的に暗号化し、かつ暗号化箇所を見つけ難くした処理を施すことによって、音楽や映像情報等の不正使用を防止する暗号化情報伝送方法、伝送装置、及び伝送媒体を提供することを目的とする。

【０００２】

【従来の技術】昨今の圧縮技術の進歩により、インターネットのような低レートな回線でも音楽や映像信号を高品位で伝送することが可能となってきている。このような背景をもとに、音楽や映像などの情報配信ビジネスが急速に普及しつつある。インターネットを利用して、簡単に高品位な音楽や映像情報を入手できることは大変便利ではあるが、一方ではこれらの情報を著作権者の許可なく大量に複写するなどの不正使用が問題となってい

る。

【０００３】音楽や映像等の情報の不正複写を防止する方法としては、情報そのものを暗号化する方法が従来から数多く採用されている。つまり、暗号化に使用した鍵が解らなければ、仮に不正に複写されても元の情報に戻せないので、結果的に全く意味のない複写としてしまう方式である。

【０００４】図３に、従来より行われている暗号化手法を用いた情報伝送の一例を示す。ユーザー（受信側）とプロバイダー（送信側）との回線接続が行われると、まず最初に認証処理がなされる（ステップ１）。認証の結果、受信側が正規ユーザーではない（ＮＧ）と判定されると、当然のことであるが、そこで回線が遮断される。正規ユーザーである（ＯＫ）と判定されると、コンテンツ情報を暗号化するときに使用したキー（鍵）と暗号化された音楽、映像等のコンテンツ情報がユーザー側に伝送される（ステップ２～４）。

【０００５】ここで、コンテンツ情報を暗号化する際に使用したキーの伝送であるが、キーもそのままの状態（裸）ではなく、何らかの暗号化を施して伝送する。キーを暗号化するためのキーには特殊なデータ（ＩＤ）が使用される。例えば、受信（ユーザー）側固有のデータであるシステムＩＤとか会員番号などがある。或いは、クレジットカード番号とかキャッシュカード番号というような他人には知らせたくないデータもＩＤとして有効である。

【０００６】このようなＩＤを取得して暗号化したキーは、図３に示したようにEx(ID,Key)と表現される。音楽情報や映像情報を暗号化するためのキーであるKeyを、前述したIDをキーとして、ある暗号化方式Ex()で暗号化するということを意味している。同様な式を用いて音楽や映像情報（Data）の暗号化を表現すると、Ey(Key,Data)となる。

【０００７】受信側には暗号化されたキーである Ex(ID,Key)と、暗号化された音声や映像の情報である Ey(Key,Data)が記憶されることになる。何れのデータも暗号化されており、仮に不正に複写されても簡単には元の音楽や映像情報に戻すことができないわけである。以上が、従来よりの情報の不正使用を防止するために採られている方式の概要である。

【０００８】

【発明が解決しようとする課題】ところで、ユーザの購入意欲を高めるに、購入対象となる音楽や映像の一部を、たとえ品質が悪い状態でも自由に再生できるようにしておくこと（暗号化しない状態のままにしておくこと）は、いろいろな面で有利である。ここで問題となるのが、不正使用を防止するために、コンテンツ全体に暗号化を施した場合には、暗号を完全に解かない限り、全く音楽や映像を再生することができないことである。

【０００９】一方、暗号を解かなくてもある程度の品質で部分的な再生を可能とするために、部分的に暗号化を施した場合には、従来、ストリームのどの部分が暗号化されているか否かの情報（フラッグ）を、伝送されるストリーム内部に設けていた。よって、コンテンツ全体を元の情報に戻しやすくなり、不正使用を防止する能力が低下するといった問題があった。

【００１０】この発明は、音声や画像等の伝送ストリームの部分的なある程度の品質での再生を、暗号を解かなくても可能とするために、伝送ストリームを部分的に暗号化した場合においても、コンテンツの不正使用を強力に防止できる暗号化情報伝送方法、伝送装置、及び伝送媒体を提供することを目的とする。

【００１１】

【課題を解決するための手段】そこで、上記課題を解決するために本発明は、下記（１）～（１０）を提供するものである。

（１）複数のフレームからなるストリームに対し、所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとを決定し、暗号化を行うと決定されたフレームのデータを各フレーム単位で暗号化してストリームを伝送することを特徴とする暗号化情報伝送方法。

（２）複数のフレームからなるストリームに対し、所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとを決定し、暗号化を行うと決定されたフレームのデータを各フレーム単位で暗号化すると共に、前記所定の生成多項式の情報を暗号化した生成多項式暗号化情報を付加してストリームを伝送することを特徴とする暗号化情報伝送方法。

（３）複数のフレームからなるストリームに対し、所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとを決定し、暗号化を行うと決定されたフレームのデータを各フレーム単位で暗号化すると共に、前記所定の生成多項式の情報を暗号化した生成多項式暗号化情報と、前記所定の生成多項式の乱数発生のための複数の初期値の情報を暗号化した初期値暗号化情報とを付加してストリームを伝送することを特徴とする暗号化情報伝送方法。

（４）複数のフレームからなるストリームに対し、所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとを決定し、暗号化を行うと決定されたフレームのデータを各フレーム単位で暗号化してストリームを伝送することを特徴とする暗号化情報伝送装置。

（５）複数のフレームからなるストリームに対し、所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとを決定し、暗号化を行うと決定されたフレームのデータを各フレーム単位で暗号化すると共に、前記所定の生成多項式

の情報を暗号化した生成多項式暗号化情報を付加してストリームを伝送することを特徴とする暗号化情報伝送装置。

（６）複数のフレームからなるストリームに対し、所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとを決定し、暗号化を行うと決定されたフレームのデータを各フレーム単位で暗号化すると共に、前記所定の生成多項式の情報を暗号化した生成多項式暗号化情報と、前記所定の生成多項式の乱数発生のための複数の初期値の情報を暗号化した初期値暗号化情報とを付加してストリームを伝送することを特徴とする暗号化情報伝送装置。

（７）複数のフレームからなるストリームに対し、所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されたストリームを伝送することを特徴とする伝送媒体。

（８）複数のフレームからなるストリームに対し、所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されると共に、前記所定の生成多項式の情報が暗号化された生成多項式暗号化情報が付加されたストリームを伝送することを特徴とする伝送媒体。

（９）複数のフレームからなるストリームに対し、所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されると共に、前記所定の生成多項式の情報が暗号化された生成多項式暗号化情報と、前記所定の生成多項式の乱数発生のための複数の初期値の情報が暗号化された初期値暗号化情報とが付加されたストリームを伝送することを特徴とする伝送媒体。

（１０）複数のフレームからなるストリームに対し、所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとを決定し、暗号化を行うと決定されたフレームのデータを各フレーム単位で暗号化すると共に、前記所定の生成多項式の乱数発生のための複数の初期値の情報を付加してストリームを伝送することを特徴とする暗号化情報伝送方法。

【００１２】

【発明の実施の形態】図１に、暗号化情報伝送方法の一実施例におけるストリームの暗号化処理方法を示す。図１（ａ）は、音声または画像ストリーム内のフレームを示している。音声データがリニアＰＣＭの場合には、ストリーム内にフレームといった概念が無い場合もあるが、数百～数千サンプル分のデータを１フレームとして、その先頭にフレーム同期信号を挿入することにより、フレームの概念を容易に導入することができる。

【００１３】また、昨今の圧縮技術の進歩により、圧縮音声や圧縮画像による伝送が伝送時間の節約のために一般的となっている。圧縮音声データの場合には、必ずフレームの概念が導入されており、固定レートによる圧縮であれば各フレームは同一サイズとなり、可変レートであればフレーム毎に異なるサイズとなる。また、圧縮画像ストリームの場合には、圧縮方式にもよるが一般的にはフレーム毎に異なるサイズとなることが多い。何れにしても、フレームのサイズは本発明内容と直接関係ないので、図１においては同一サイズで示している。

【００１４】ここで、特定の生成多項式により発生された乱数値を図１（ｂ）に示す。乱数値が「０」のときはそのフレームの暗号化は行わず、乱数値が「１」のときはそのフレームの暗号化を行うものとする。音声または画像ストリームは、図１（ｃ）に示したように、乱数値に基づきフレーム単位でランダムに暗号化される。

【００１５】このような処理を施しておけば、暗号を復元しない限り正常な音声や画像が再生されないことは明らかである。暗号化されたフレームのデータ（Data(n)）は、Ey(Key,Data(n))と表現されるので、安全強度を保つには従来方式と同じようにキー（Key）をIDを用いて暗号化する。暗号化されたキー情報は、Ex(ID,Key)と表現され、安全強度は従来方式と同じである。ここでの特徴点は、フレーム単位で暗号化されているか否かである。仮に、キー（Key）が盗まれたとしても、ストリームのフレーム毎に暗号を解くか否かの手作業的な処理が要求されるので、情報全体を完全な元の状態に戻すには、かなりの手間が必要となることは明らかである。このように、本実施例は暗号化されている部分が何処であるか見つけ出し難くしているので、コンテンツの不正使用に対する安全強度を、従来の部分的な暗号化方法よりも高めることができる。

【００１６】次に、暗号化を行うか否かの決定に使用される乱数発生について説明する。乱数の発生は、衆知の如く、特定の生成多項式に基づくＭ系列信号発生器やソフト処理で容易に実現できるので、詳細説明は省くが、生成多項式の次数については安全性を確保する意味で、次のような点を考慮して決定するとよい。

【００１７】今、生成多項式の次数をｍとすると、発生される乱数は2^m-1回で巡回する。従って、「2^m-1」が音声や画像ストリームの総フレーム数より十分大きな値となるように、次数ｍを設定することが望ましい。例えば、２時間のコンテンツで、フレーム周波数を１００Ｈｚとすると、総フレーム数は、７２００秒ｘ１００＝７２０ｋとなる。従って、ｍは２０以上にすれば十分である。次数ｍが高くなればなるほど、乱数を発生できる特定の生成多項式の種類も増えるので、例えばｍ＝２０であるとすると、実際に使用されている生成多項式を見つけだすことはもはや不可能に近い状況となる。

【００１８】本実施例では、安全強度を高めるために、乱数発生のための生成多項式についても暗号化して伝送することを特長としている。生成多項式タイプの暗号化は、Ez(ID,生成多項式)と表現できる。ここでの暗号化方式 Ez()は、キー（Key）を暗合化するときの暗号化方式Ex()と同じにしても問題は無いが、少しでも安全強度を高めようとするならば、暗号アルゴリズムを変えることも可能である。

【００１９】以上のように、本実施例における音声・画像等のストリームの暗号化伝送方法は、ストリームを全体でなく部分的に暗号化し、かつ、どのフレームが暗号化されているか否かを示すフラッグ情報などをストリーム内に設けずに、特定の生成多項式により発生される乱数を基に、該当フレームを暗号化するか否かを決定すしている。さらに、安全性を確保するために、使用された生成多項式に関する情報を暗号化して受信側に伝送する。

【００２０】これらの処理のフローを、図２に示す。図２において、キー（Key）を暗号化したデータEx(ID,Key)、音声や画像ストリームを暗号化したデータEy(Key,Data(n))に加えて、乱数発生のための生成多項式のタイプを暗号化したデータEz(ID,生成多項式)を受信側に伝送している。なお、図２のステップ１４には「乱数発生のための初期値表の伝送」が記載されているが、これについては詳細を後述する。

【００２１】図２について簡単に説明すると、ユーザー（受信側）とプロバイダー（送信側）との回線接続が行われると、まず最初に認証処理がなされる（ステップ１）。認証の結果、受信側が正規ユーザーではない（ＮＧ）と判定されると、当然のことであるが、そこで回線が遮断される。正規ユーザーである（ＯＫ）と判定されると、ステップ１２において、キー（Key）及び生成多項式のタイプを暗号化するためのキー(ID)を取得し、キー（Key）及び生成多項式のタイプを暗号化したデータEx(ID,Key)とEz(ID,生成多項式)を得る。ステップ１３において、音声・画像等のコンテンツ情報を暗号化したデータEy(Key,Data(n))を取得、または、乱数を発生させてデータEy(Key,Data(n))を生成する。ステップ１４において、コンテンツ情報を暗号化したデータ（図１（Ｃ）に示すように暗号化されていないフレームのデータも当然含むもの）であるEy(Key,Data(n))に加えて、Ex(ID,Key)とEz(ID,生成多項式)、さらには乱数発生のための初期値表（乱数発生のための複数の初期値）のデータを受信側に伝送する。

【００２２】なお、キー（Key）を暗号化したデータEx(ID,Key)、乱数発生のための生成多項式のタイプを暗号化したデータEz(ID,生成多項式)において、暗号化のためのキーは同じＩＤとなっているが、お互いに異なる情報を用いてもかまわないので、例えば、Ex(ID,Key)のIDにはシステムＩＤを、Ez(ID,生成多項式)のIDにはキャッシュカード番号を使用するといった方法が考えられる。

【００２３】伝送側から受信側（再生側）への情報の受け渡しを行う伝送媒体としては、暗号化された音声や画像の伝送ストリームEy(Key,Data(n))が圧縮情報であっても大きな容量であるため、回線（光ケーブル、電気信号ケーブル等）ばかりでなく、光ディスクや磁気記録媒体といった記録媒体でもよい。

【００２４】図２に示す処理を実現する暗号化情報伝送装置としては、複数のフレームからなるストリームに対し、所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとを決定する手段と、暗号化を行うと決定されたフレームのデータを各フレーム単位で暗号化する手段と、前記所定の生成多項式の情報を暗号化した生成多項式暗号化情報を生成する手段と、前記所定の生成多項式の乱数発生のための複数の初期値の情報を暗号化した初期値暗号化情報を生成する手段と、部分的に暗号化を行ったストリームと生成多項式暗号化情報と初期値暗号化情報とを伝送する手段を備えた暗号化情報伝送装置が考えられる。

【００２５】ところで、前述したようにストリームをフレーム単位で部分的に暗号化し、かつ暗号化されているフレームであるか否かを示すフラッグ情報などをストリーム内に設けない方法は、不正使用に対する安全強度という面では大変優れている。但し、ストリームの途中から再生する場合には次のような不利な面がある。即ち、暗号化するか否かを決定する乱数の発生はフレーム単位で連続的に行われるため、いきなりストリームの途中から再生しようとすると、ストリームの最初のフレームから途中のフレームまで（即ち再生を開始するフレームまで）の乱数発生を短時間に行わなければならない。これは、非常に難しい。

【００２６】この問題を解決するために、本実施例では、前述した図２のステップ１４に示したように、前もって算出した乱数発生のための初期値を複数個用意し（初期値表を用意し）、受信側へ伝送する。例えば、１００フレーム毎、即ち仮にフレーム周波数が１００Ｈｚであれば、１秒単位での乱数値となる。一つの初期値は、乱数発生のための生成多項式の次数をｍとすると、ｍビットのサイズであるので、例えば、２時間のコンテンツに対しては、初期値表は７２００＊ｍビットとなる。ストリームの途中から再生する場合、フレームアドレスとかタイムコードなどにより、現在のフレームが最初から何フレーム目であるかが容易に分かるので、初期値表から最適な初期値を選択し乱数発生器に設定すれば、極僅かなステップ数で乱数発生器を所望の状態にもっていくことが可能となる。

【００２７】このようにして、ストリームを部分的に暗号化し、かつ暗号化されているフレームであるか否かを

示すフラッグ情報などをストリーム内に設けない方法でも、ストリームの任意の位置よりの再生が可能となる。なお、これら複数の初期値（初期値表）を受信側へ伝送するとき、そのまま伝送してもよいが、暗号化して伝送した方がより安全であることは確かである。

【００２８】以上の説明は、ストリームを部分的に暗号化し、かつ暗号化されているフレームであるか否かを示すフラッグ情報などをストリーム内に設けない伝送方法において、ストリームの途中から再生することを容易に可能とするために、送信側より乱数発生のための初期値表を伝送するという方法を紹介した。

【００２９】正規のユーザーである受信側（再生側）で乱数発生のための生成多項式が事前に分かっている場合には、伝送ストリームの再生に先立って初期値表を作成することが可能である。或いは、初期値表でなく乱数値そのものを作成することも可能である。というのは、乱数値は「０」か「１」の１ビットであるので、総フレーム分の乱数表を作成しても実現可能なサイズである。例えば、２時間のコンテンツで、フレーム周波数を１００Ｈｚとすると、総フレーム数は７２００ｘ１００＝７２０ｋビット＝９０ｋバイトとなる。

【００３０】一方、前述した初期値表の場合には、生成多項式の次数ｍ＝２０とし、１００フレーム毎の初期値表を作成しようとすると、７２００ｘ１００ｘ２０／１００ビット＝１８ｋバイトとなる。受信側（再生側）でのメモリーサイズの面からすると、初期値表を伝送或いは作成した方が優れているが、受信側で生成する総フレームに対応した乱数表の方が使い勝手に優れていると思われる。いずれにしても、不正使用に対する安全強度を確保しつつ、伝送ストリームの途中からの再生を容易に行える。

【００３１】ここで、上述した伝送ストリームの再生方法（受信方法）については次のような方法が考えられる。

（イ）所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されたストリームを再生する暗号化情報再生方法であって、前記所定の生成多項式を用いて発生される乱数に基づき、暗号化されたフレームと暗号化されていないフレームとを特定した後に、ストリームの再生を行うことを特徴とする暗号化情報再生方法。

（ロ）所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されると共に、前記所定の生成多項式の情報が暗号化された生成多項式暗号化情報が付加されたストリームを再生する暗号化情報再生方法であって、前記生成多項式暗号化情報の暗号を解き、得られた前記生成多項式を用いて発生される乱数に基づき、暗号化されたフレームと暗号化されていないフレームとを特定した後に、ストリームの再生を行うことを特徴とする暗号化情報再生方法。

（ハ）所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されると共に、前記所定の生成多項式の情報が暗号化された生成多項式暗号化情報と、前記所定の生成多項式の乱数発生のための複数の初期値の情報が暗号化された初期値暗号化情報とが付加されたストリームを再生する暗号化情報再生方法であって、前記生成多項式暗号化情報の暗号を解き前記生成多項式を復元すると共に、前記初期値暗号化情報の暗号を解き前記初期値を復元し、復元された前記生成多項式を用いて発生される乱数と、復元された前記初期値とに基づき、暗号化されたフレームと暗号化されていないフレームとを特定した後に、ストリームの再生を行うことを特徴とする暗号化情報再生方法。

（ニ）所定の生成多項式を用いて発生される乱数に基づき、暗号化を行うフレームと暗号化を行わないフレームとが決定され、暗号化を行うと決定されたフレームのデータが各フレーム単位で暗号化されると共に、前記所定の生成多項式の乱数発生のための複数の初期値の情報が付加されたストリームを再生する暗号化情報再生方法であって、前記初期値の情報を再生して前記初期値を得、前記生成多項式を用いて発生される乱数と、再生した前記初期値とに基づき、暗号化されたフレームと暗号化されていないフレームとを特定した後に、ストリームの再生を行うことを特徴とする暗号化情報再生方法。

【００３２】また、上記の再生方法を実現する暗号化情報再生装置としては、前記生成多項式暗号化情報の暗号を解き前記生成多項式を復元する手段と、前記初期値暗号化情報の暗号を解き前記初期値を復元する手段と、復元された前記生成多項式を用いて発生される乱数と、復元された前記初期値とに基づき、暗号化されたフレームと暗号化されていないフレームとを特定する手段と、フレーム毎の暗号化の有無が特定されたた後にその暗号化の有無の情報に基づき、ストリームの再生を行う手段をを備えた暗号化情報再生装置が考えられる。

【００３３】

【発明の効果】以上の通り、本発明によれば、音声や画像等のコンテンツ情報全体を暗号化せずに部分的かつランダムに暗号化し、しかも、暗号化されている部分がどの部分であるかを見つけ出し難くしているので、コンテンツの不正使用に対する安全強度を高めることができる。また、コンテンツ情報全体を暗号化せずに部分的かつランダムに暗号化しているので、ある程度の品質での部分的な再生が自由に行え、ユーザーの購入意欲を増加させることにとって大変有利である。さらには、所定の

11

生成多項式の乱数発生のための複数の初期値の情報を付加して伝送する場合には、再生時において、不正使用に対する安全強度を確保しつつ、伝送ストリームの途中からの再生を容易に行える。

【図面の簡単な説明】

12

【図１】本発明における暗号化情報伝送方法の一実施例のストリームの暗号化処理を示す図である。

【図２】本発明における暗号化情報伝送方法の一実施例の処理フローを示す図である。

【図３】従来の暗号化情報伝送方法を示す図である。

【図１】

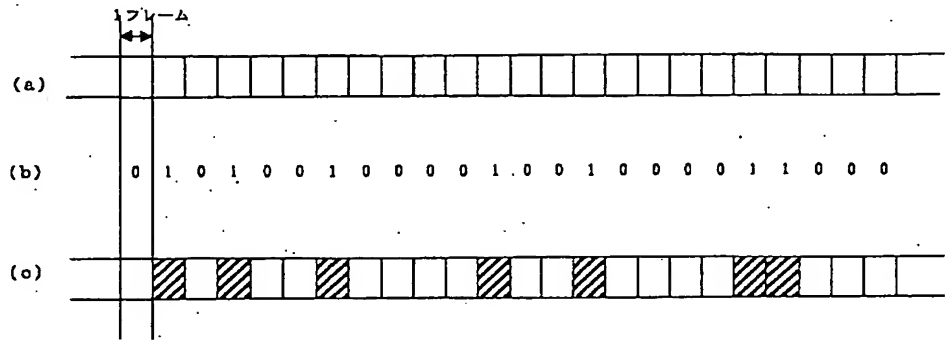


図1

【図２】

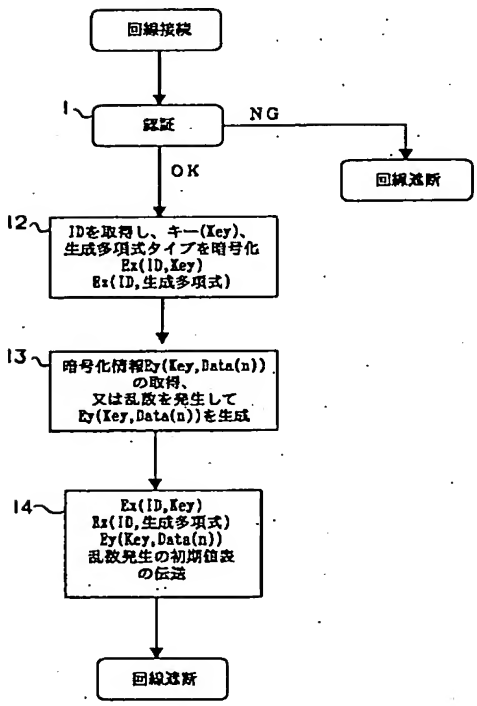


図2

【図３】

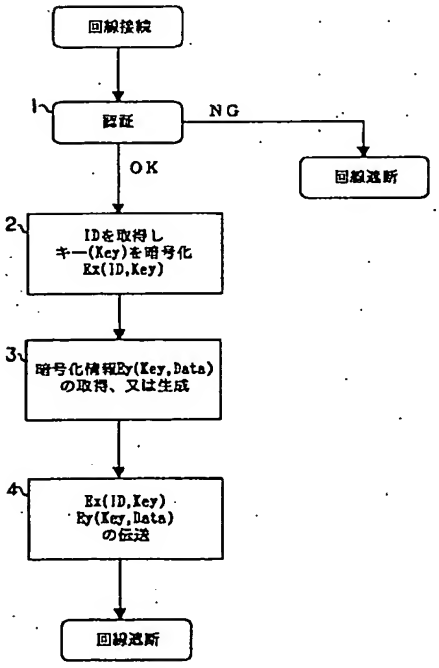


図3